UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/601,591	09/25/2000	Jerome Meric	11345.024001	8352

22511 7590 11/02/2006

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
HOYE, MICHAEL W	

ART UNIT	PAPER NUMBER
2623	

DATE MAILED: 11/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/601,591	MERIC ET AL.	
	Examiner	Art Unit	
	Michael W. Hoye	2623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicants' arguments, see pages 8-12, filed on August 24, 2006, with respect to claims 1-40 have been considered but are moot in view of the new ground(s) of rejection, see below.

2. Regarding the Newby et al. patent (US 5,796,829), the Applicants argue on pages 10-11 that, "the conditional access processes disclosed in Newby relate to processes for decryption of received information segments that are executed on a single conditional access system...Thus, Newby fails to disclose or suggest configuring a filter to extract specific components of received data based on one conditional access system of a plurality of conditional access systems" (see Remarks, pg. 12, paragraph 2).

In response, the examiner respectfully disagrees. The Newby et al. reference specifically discloses:

> "an access control processor for a conditional access system in which encrypted information segments provided by a plurality of information service providers are encrypted for transmission in accordance with different conditional access processes respectively utilizing different algorithms for encrypting the information segments...and a conditional access controller in the information receiver for selectively enabling the decryptor to decrypt received information segments encrypted in accordance with any of said different conditional access processes by providing to the decryptor cryptographic information for defining the algorithm utilized in said one of said different conditional access processes for use by the decryptor to decrypt the received information segment encrypted in accordance with said algorithm" (see Newby Abstract and 2:48-3:1).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7, 12-13, 16-22, 27-29, 33-36 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (US 2002/0044658 A1 of record), in view of Newby et al. (US 5,796,829 of record), in further view of Tamer et al. (US 6,671,881 B1 of record).

As to claim 1, note the Wasilewski et al. reference that discloses a conditional access system. Regarding the claimed "A device for use in a receiver/decoder operable with **a plurality of different conditional access systems**", the Wasilewski et al. reference discloses a conditional access system with different types of conditional access messages wherein the headers contain an identifier for the conditional access system and an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents (Wasilewski et al. [0161-0165]; Provisional '575 [27:10-20]) wherein "in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services" (Wasilewski et al. [00139]; Provisional '575 [24:20-25:8]). However, the Wasilewski et al. reference does not specifically disclose, "a receiver/decoder operable with a plurality of different conditional access systems." Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides

appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process used is used to retrieve cryptographic information from memory (Newby 9:1-41). In addition, Newby specifically teaches that the encrypted information segments are provided by a plurality of information service providers and encrypted for transmission in accordance with different conditional access processes respectively using different algorithms for encrypting the information segments (Newby Abstract and 2:48-3:1). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. operability with different conditional access systems for the purpose of allowing the decryptor to correctly decrypt information by using the correct conditional access system and allowing a receiver/decoder to receive media from a plurality of service providers while maintaining flexibility by allowing different service providers to use different conditional access schemes (Newby 11:1-14). The claimed "means for manipulating data received by the receiver/decoder according to a manipulation protocol" is met by "DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 for decrypt and descramble services" (Wasilewski et al. [0139]; Provisional '575 [23:20-24:8]). The claimed manipulation protocol "which is configurable in dependence on a particular one of the plurality

of different conditional access systems" is met by "EMMs that modify an entitlement agent's authorization information are made in response to modification information 403 provided by the entitlement agent or required by the network operator...The EA modification information 403 contained in the EMM goes, however, to EMM manager 407, which uses the information to modify the authorization information for the entitlement agent in DHCT 333" (Wasilewski et al. [0089]; Provisional '575 [16:1-11]), and by the Wasilewski et al. and Newby et al. combination as discussed above wherein parameters corresponding to a conditional access system used in the received stream are retrieved. The claimed "means for storing parameters associated with the manipulation protocol" is met by "...storage provides a place to store the entitlement agent's public key, the authorization information for the services and service instances provided by the entitlement agent, and the MSKs provided by the entitlement agent" (Wasilewski et al. [0091]; Provisional '575 [16:25-17:8]). The claimed "means for receiving a command instructing configuration of the manipulation protocol in dependence on the particular one of the plurality of different conditional access systems" is met by EA modification information for modifying the authorization information for the entitlement agent in DHCT 333 (Wasilewski et al. [0089]; Provisional '575 [16:7-9), as well as the Wasilewski et al. and Newby et al. combination as discussed above. The claimed "means for retrieving a parameter from the storage means in dependence on the command" is met by the EA modification information used for modifications including adding or canceling services provided by the entitlement authority and changing the conditions under which access to instances of a given service will be granted (Wasilewski et al. [0089]; Provisional '575 [16:7-11]) wherein retrieval of such data is inherent to its modification. The claimed "means for outputting said parameter to the manipulation means for use in

configuring the manipulation protocol, whereby the manipulation means is not required to receive all parameters necessary to configure the manipulation protocol in dependence on all of the conditional access systems" is met by "DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625" (Wasilewski et al. [0139]; Provisional '575 [24:20-25:8]). Also note, that Wasilewski et al. reference discloses that the DHCTSE is functionally equivalent to a smart card wherein "DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a 'smart card'" (Wasilewski et al. [0190]). However, the Wasilewski et al. reference does not specifically disclose "wherein the manipulation means comprises a demultiplexer and a filter configured to filter the data received by the receiver/decoder, and wherein the manipulation protocol changes the filter to extract specific components of the received data." Now note the Tamer et al. reference discloses a conditional access filter as for a packet video signal inverse transport system. The claimed "wherein the manipulation means comprises a demultiplexer" is met by "[t]he detected frequency band may contain a plurality of time division multiplexed programs in packet form. To be useful, only packets from a single program should be passed to the further circuit elements...The programmable registers and the received SCID register are coupled to respective input ports of a comparator circuit 15, and the received SCID is compared...If the SCID for a packet matches...the comparator 15 conditions a memory controller 17 to route that packet to a predetermined location..." (Tamer 3:26-53), such functionality equivalent and thus meeting to the claimed demultiplexer. The claimed "[wherein the manipulation means comprises] a filter

configured to filter the data received by the receiver/decoder, and wherein the manipulation protocol changes the filter to extract specific components of the received data" is met by "[a] further layer of coding may be instantly impressed on the entitlement information by including a conditional access code to permit/prohibit reception of the EMM and ECM data within respective packets, and thereby allow substantially instant permission/prohibition to certain programs...A matched filter or E-code decoder 30, is arranged to detect a subscriber specific bit pattern within the 128 bit header. If a match is detected the decoder communicates with the memory controller 17 and the smart card 31 to make the remainder of the entitlement payload available...The conditional access codes may be periodically changed if the matched filter 30 is made programmable. These codes may be periodically provided by the smart card" (Tamer 5:1-31) wherein it is inherent that this process be "based on the particular one of the plurality of different conditional access system" in order to successfully extract components of the received data. Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. and Newby et al. receipt of EMM and ECM data by DHCTSE (smart card equivalent) with the Tamer et al. demultiplexer and filter programmable by smart card for the purpose of "allow[ing] substantially instant permission/prohibition to certain programs" (Tamer 5:10-11) and the receipt of programming using a transmission scheme capable of transmitting a greater number of programming choices.

As to claim 2, the claimed "arranged to output said parameter to the manipulation means upon receipt of a command instructing output of said parameter" is met by DHCTSE referring to stored entitlement information to determine if DHCT has an entitlement to receive the instance

of service which the ECM accompanies wherein the DHCTSE processes the ECM if authorized (Wasilewski et al. [0139]; Provisional '575 [24:20-25:8]).

As to claim 3, the claimed "comprising means for receiving a command notifying the device of updating of the parameters stored in the storage means" is met by "[t]he task of EMM manager 407 is to respond to EMMs which add or remove entitlement agents and to EMMs which modify the authorizations for an entitlement agent" (Wasilewski et al. [0088]; Provisional '575 [15:18-29]).

As to claim 4, the claimed "wherein said parameters include an identifier of the particular one of the plurality of conditional access systems currently being used by the receiver/decoder." Note the Wasilewski et al. reference discloses a conditional access system with different types of conditional access messages wherein the headers contain an identifier for the conditional access system and an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents (Wasilewski et al. [0161-0165]; Provisional '575 [27:10-20]) wherein "in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services" (Wasilewski et al. [00139]; Provisional '575 [24:20-25:8]). However, the Wasilewski et al. reference is silent as to the ECM processing method. Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt

the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process used is used to retrieve cryptographic information from memory (Newby 9:1-41). In addition, as stated above, Newby specifically teaches that the encrypted information segments are provided by a plurality of information service providers and encrypted for transmission in accordance with different conditional access processes respectively using different algorithms for encrypting the information segments (Newby Abstract and 2:48-3:1). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. conditional access system ID for the purpose of allowing the decryptor to correctly decrypt information by using the correct conditional access system.

As to claim 5, please see rejection of claim 4.

As to claim 6, the claimed "wherein the device is capable of receiving commands from a configuring application" is met by "[t]he task of EMM manager 407 is to respond to EMMs which add or remove entitlement agents and to EMMs which modify the authorizations for an entitlement agent" (Wasilewski et al. [0088]; Provisional '575 [15:18-29]).

As to claim 7, the claimed "wherein the device is capable of changing an identifier of the particular one of the plurality of different conditional access systems currently being used by the receiver/decoder in response to a command from the configuring application." Note the Wasilewski et al. reference discloses a conditional access system with different types of conditional access messages wherein the headers contain an identifier for the conditional access

system and an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents (Wasilewski et al. [0161-0165]; Provisional '575 [27:10-20]) wherein "in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services" (Wasilewski et al. [00139]; Provisional '575 [24:20-25:8]). However, the Wasilewski et al. reference is silent as to the ECM processing method. Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process is used to retrieve cryptographic information from memory (Newby 9:1-41). In addition, as stated above, Newby specifically teaches that the encrypted information segments are provided by a plurality of information service providers and encrypted for transmission in accordance with different conditional access processes respectively using different algorithms for encrypting the information segments (Newby Abstract and 2:48-3:1). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. conditional access system ID for the purpose of allowing the

decryptor to correctly decrypt information by using the correct conditional access system. Also note that a change occurs when the system decrypts a new stream of data that is encrypted using a different conditional access system.

As to claim 12, the claimed "arranged to receive requests from a plurality of client applications for a plurality of parameters" is met by "applications running on DHCT 333 which use the conditional access system and DHCTSE 627" (Wasilewski et al. [0137]; Provisional '575 [23:15-18]) wherein DHCTSE 627 provides encryption, decryption, digest, and digital signature services for such applications executing on DHCT (Wasilewski et al. [0139]; Provisional '575 [23:20-24:8]) with associated parameters.

As to claim 13, the claimed "said manipulation means arranged to operate under the control of the device to manipulate data" is met by using entitlement information to determine whether DHCT receiving the ECM has an entitlement of the instance of service and, if authorized, processing ECM data and providing the control word to a service decryptor module (Wasilewski et al. [00139]; Provisional '575 [23:20-24:8]). The claimed "and said means for storing parameters is associated with the manipulation protocol" is met by memory containing keys, entitlement information, and executable code (Wasilewski et al. [0192-0195]; Provisional '575 [33:3-34:7]).

As to claim 16, note the Wasilewski et al. reference that discloses a conditional access system. The claimed "means for manipulating data received by the receiver/decoder according to a manipulation protocol" is met by "DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides

the control word to service decryptor module 625 for decrypt and descramble services" (Wasilewski et al. [0139]; Provisional '575 [23:20-24:8]). The claimed manipulation protocol "which is configurable in dependence on a particular one of a plurality of conditional access systems" is met in part by "EMMs that modify an entitlement agent's authorization information are made in response to modification information 403 provided by the entitlement agent or required by the network operator...The EA modification information 403 contained in the EMM goes, however, to EMM manager 407, which uses the information to modify the authorization information for the entitlement agent in DHCT 333" (Wasilewski et al. [0089]; Provisional '575 [16:1-11]). However, the Wasilewski et al. reference does not specifically disclose, "in dependence on a particular one of a plurality of conditional access systems." Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process used is used to retrieve cryptographic information from memory (Newby 9:1-41). In addition, Newby specifically teaches that the encrypted information segments are provided by a plurality of information service providers and encrypted for transmission in accordance with different conditional access processes respectively using different algorithms for encrypting the information segments (Newby Abstract and 2:48-3:1). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the

art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. operability with different conditional access systems for the purpose of allowing the decryptor to correctly decrypt information by using the correct conditional access system and allowing a receiver/decoder to receive media from a plurality of service providers while maintaining flexibility by allowing different service providers to use different conditional access schemes (Newby 11:1-14). The claimed "means for storing parameters associated with the manipulation protocol" is met by "...storage provides a place to store the entitlement agent's public key, the authorization information for the services and service instances provided by the entitlement agent, and the MSKs provided by the entitlement agent" (Wasilewski et al. [0091]; Provisional '575 [16:25-17:8]). The claimed "receiving a command instructing configuration of the manipulation protocol in dependence on the particular conditional access system" is met by EA modification information for modifying the authorization information for the entitlement agent in DHCT 333 (Wasilewski et al. [0089]; Provisional '575 [16:1-11]), as well as the Wasilewski et al. and Newby et al. combination as discussed above. The claimed "retrieving a parameter from the storage means in dependence on the command" is met by the EA modification information used for modifications including adding or canceling services provided by the entitlement authority and changing the conditions under which access to instances of a given service will be granted (Wasilewski et al. [0089]; Provisional '575 [16:1-11]) wherein retrieval of such data is inherent to its modification. The claimed "outputting said parameter to the manipulation means for use in configuring the manipulation protocol, whereby the manipulation means is not required to receive all parameters necessary to configure the manipulation protocol in dependence on the plurality of conditional access systems" is met by

"DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625" (Wasilewski et al. [0139]; Provisional '575 [23:20-24:8]), as well as the Wasilewski et al. and Newby et al. combination as discussed above. Also note, that Wasilewski et al. reference discloses that the DHCTSE is functionally equivalent to a smart card wherein "DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a 'smart card'" (Wasilewski et al. [0190]). However, the Wasilewski et al. reference does not specifically disclose "wherein the manipulation means comprises a demultiplexer and a filter configured to filter the data received by the receiver/decoder, and wherein the manipulation protocol changes the filter to extract specific components of the received data." Now note the Tamer et al. reference discloses a conditional access filter as for a packet video signal inverse transport system. The claimed "wherein the manipulation means comprises a demultiplexer" is met by "[t]he detected frequency band may contain a plurality of time division multiplexed programs in packet form. To be useful, only packets from a single program should be passed to the further circuit elements...The programmable registers and the received SCID register are coupled to respective input ports of a comparator circuit 15, and the received SCID is compared...If the SCID for a packet matches...the comparator 15 conditions a memory controller 17 to route that packet to a predetermined location..." (Tamer 3:26-53), such functionality equivalent and thus meeting to the claimed demultiplexer. The claimed "[wherein the manipulation means comprises] a filter configured to filter the data received by the receiver/decoder, and wherein the manipulation protocol changes the filter to extract specific

components of the received data" is met by "[a] further layer of coding may be instantly impressed on the entitlement information by including a conditional access code to permit/prohibit reception of the EMM and ECM data within respective packets, and thereby allow substantially instant permission/prohibition to certain programs...A matched filter or E-code decoder 30, is arranged to detect a subscriber specific bit pattern within the 128 bit header. If a match is detected the decoder communicates with the memory controller 17 and the smart card 31 to make the remainder of the entitlement payload available...The conditional access codes may be periodically changed if the matched filter 30 is made programmable. These codes may be periodically provided by the smart card" (Tamer 5:1-31) wherein it is inherent that this process be "based on the particular conditional access system" in order to successfully extract components of the received data. Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. receipt of EMM and ECM data by DHCTSE (smart card equivalent), as combined with Newby et al, with the Tamer et al. demultiplexer and filter programmable by smart card for the purpose of "allow[ing] substantially instant permission/prohibition to certain programs" (Tamer 5:10-11) and the receipt of programming using a transmission scheme capable of transmitting a greater number of programming choices.

As to claim 17, the claimed "wherein said parameter is output upon receipt of a command instructing output of said parameter" is met by DHCTSE referring to stored entitlement information to determine if DHCT has an entitlement to receive the instance of service which the ECM accompanies wherein the DHCTSE processes the ECM if authorized (Wasilewski et al. [0139]; Provisional '575 [23:20-24:8]).

As to claim 18, the claimed "comprising the step of receiving a command notifying the device of updating of the parameters stored in the storage means" is met by "[t]he task of EMM manager 407 is to respond to EMMs which add or remove entitlement agents and to EMMs which modify the authorizations for an entitlement agent" (Wasilewski et al. [0088]; Provisional '575 [15:18-29]).

As to claim 19, the claimed "wherein said parameters include an identifier of the conditional access system currently being used by the receiver/decoder." Note the Wasilewski et al. reference discloses a conditional access system with different types of conditional access messages wherein the headers contain an identifier for the conditional access system and an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents (Wasilewski et al. [0161-0165]; Provisional '575 [27:10-20]) wherein "in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services" (Wasilewski et al. [00139]; Provisional '575 [24:20-25:8]). However, the Wasilewski et al. reference is silent as to the ECM processing method. Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access

process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process used is used to retrieve cryptographic information from memory (Newby 9:1-41). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. conditional access system ID for the purpose of allowing the decryptor to correctly decrypt information by using the correct conditional access system.

As to claim 20, please see rejection of claim 19.

As to claim 21, the claimed "wherein commands are received from a configuring application" is met by "[t]he task of EMM manager 407 is to respond to EMMs which add or remove entitlement agents and to EMMs which modify the authorizations for an entitlement agent" (Wasilewski et al. [0088]; Provisional '575 [15:18-29]).

As to claim 22, the claimed "wherein an identifier of the particular conditional access system currently being used by the receiver/decoder is changed in response to a command from the configuring application." Note the Wasilewski et al. reference discloses a conditional access system with different types of conditional access messages wherein the headers contain an identifier for the conditional access system and an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents (Wasilewski et al. [0161-0165]; Provisional '575 [27:10-20]) wherein "in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module

625 in a form that it may use to decrypt or descramble services" (Wasilewski et al. [00139]; Provisional '575 [24:20-25:8]). However, the Wasilewski et al. reference is silent as to the ECM processing method. Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process is used to retrieve cryptographic information from memory (Newby 9:1-41). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. conditional access system ID for the purpose of allowing the decryptor to correctly decrypt information by using the correct conditional access system. Also note that a change occurs when the system decrypts a new stream of data that is encrypted using a different conditional access system.

As to claim 27, the claimed "wherein requests are received from a plurality of client applications for a plurality of parameters" is met by "applications running on DHCT 333 which use the conditional access system and DHCTSE 627" (Wasilewski et al. [0137]; Provisional '575 [23:15-18]) wherein DHCTSE 627 provides encryption, decryption, digest, and digital signature services for such applications executing on DHCT (Wasilewski et al. [0139]; Provisional '575 [23:20-24:8]) with associated parameters.

As to claim 28, note the Wasilewski et al. reference that discloses a conditional access system. The claimed "receiver/decoder including means for storing parameters associated with manipulating data received by the receiver/decoder" is met by "EA modification information 403 contained in the EMM goes, however, to EMM manager 407, which uses the information to modify the authorization information for the entitlement agent in DHCT 333...modifications include adding or canceling services provided by the entitlement authority and changing the conditions under which access to instances of a given service will be granted" (Wasilewski et al. [0089]; Provisional '575 [16:1-11]) wherein "storage provides a place to store the entitlement agent's public key, the authorization information for the services and service instances provided by the entitlement agent, and the MSKs provided by the entitlement agent" (Wasilewski et al. [0091]; Provisional '575 [16:25-17:8]). The claimed "and at least one application or further device" is met by executable code for performing processes necessary for the receiver/decoder to view conditional access information, wherein code is contained in memory (Wasilewski et al. [0191-0196]; Provisional '575 [32:21-34:17]). Note, the Wasilewski et al. reference discloses conditional access messages including an identifier for the conditional access system and an identifier for the type of security algorithm used with the message (Wasilewski et al. [0160-0168]; Provisional '575 [27:10-28:4]). However, the Wasilewski et al. reference is silent as to the generation and outputting of an identifier. Now note, the Newby et al. reference that also discloses a conditional access system. The claimed "means for outputting said identifier to said at least one application or further device" is met by "[i]n the conditional access controller of Fig. 4, the status signal 84 includes both an enable signal and data identifying either condition access process A or conditional access process B as the conditional access process used for encrypting

the information segment identified in the service request signal 40" wherein the corresponding cryptographic data is retrieved from memory (Newby 9:1-41) wherein it is inherent that an identifier be generated for the at least one parameter for successful retrieval. Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. conditional access system with plural conditional access systems and security algorithms with the Newby et al. identifiers for the purpose of providing a means for processing received data signals using difference conditional access systems efficiently. Also note, that Wasilewski et al. reference discloses that the DHCTSE is functionally equivalent to a smart card wherein "DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a 'smart card'" (Wasilewski et al. [0190]). However, the Wasilewski et al. reference does not specifically disclose "wherein manipulating data received by the receiver/decoder comprises filtering the received data to extract specific components of the received data." Now note the Tamer et al. reference discloses a conditional access filter as for a packet video signal inverse transport system. The claimed "wherein manipulating data received by the receiver/decoder comprises filtering the received data to extract specific components of the received data and wherein filtering is through a filter configurable" is met by "[a] further layer of coding may be instantly impressed on the entitlement information by including a conditional access code to permit/prohibit reception of the EMM and ECM data within respective packets, and thereby allow substantially instant permission/prohibition to certain programs...A matched filter or E-code decoder 30, is arranged to detect a subscriber specific bit pattern within the 128 bit header. If a match is detected the decoder communicates with the memory controller 17 and the smart

card 31 to make the remainder of the entitlement payload available...The conditional access codes may be periodically changed if the matched filter 30 is made programmable. These codes may be periodically provided by the smart card" (Tamer 5:1-31) wherein it is inherent that this process be "based on a particular one of a plurality of conditional access systems" in order to successfully extract components of the received data. Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. receipt of EMM and ECM data by DHCTSE (smart card equivalent) with the Tamer et al. demultiplexer and filter programmable by smart card for the purpose of "allow[ing] substantially instant permission/prohibition to certain programs" (Tamer 5:10-11).

As to claim 29, the claimed "wherein receiver/decoder is operable with the plurality of conditional access systems." Note the Wasilewski et al. reference discloses a conditional access system with different types of conditional access messages wherein the headers contain an identifier for the conditional access system and an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents (Wasilewski et al. [0161-0165]; Provisional '575 [27:10-20]) wherein "in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services" (Wasilewski et al. [00139]; Provisional '575 [24:20-25:8]). However, the Wasilewski et al. reference does not specifically disclose "wherein receiver/decoder is operable with the plurality of conditional access systems."

Now note the Newby et al. reference that discloses a conditional access system wherein upon determining that the receiver is authorized, "...conditional access controller 32 provides appropriate cryptographic information 42 to the decryptor 31 to thereby enable the decryptor 31 to decrypt the received encrypted information segments 23...cryptographic information 42 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process" (Newby 6:31-45) wherein a status signal enabling access and data identifying the conditional access process used is used to retrieve cryptographic information from memory (Newby 9:1-41). In addition, Newby specifically teaches that the encrypted information segments are provided by a plurality of information service providers and encrypted for transmission in accordance with different conditional access processes respectively using different algorithms for encrypting the information segments (Newby Abstract and 2:48-3:1). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. decryption if authorized with the Newby et al. operability with different conditional access systems for the purpose of allowing the decryptor to correctly decrypt information by using the correct conditional access system and allowing a receiver/decoder to receive media from a plurality of service providers while maintaining flexibility by allowing different service providers to use different conditional access schemes (Newby 11:1-14). The claimed "said parameters being associated with manipulating data received by the receiver/decoder according to a manipulation protocol which is configurable in dependence on the particular conditional access system" is met by the Wasilewski et al. and Newby et al. combination as discussed above wherein parameters

corresponding to a conditional access system used in the received stream are retrieved, further inv view of that discussed in the rejection of claim 28.

As to claim 33, the claimed "arranged to store a plurality of parameters, each having a respective assigned identifier" is met by that discussed in the rejection of claim 28.

As to claim 34, the claimed "said means for storing parameters associated with the manipulation of data received by the receiver/decoder, and said further device or said application" is met by the storage of manipulation parameters as discussed in the rejection of claim 28.

As to claims 35-36, please see rejections of claims 28-29.

As to claim 40, please see rejection of claim 33.

5. Claims 8-11, 14-15, 23-26, 30-32 and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (US 2002/0044658 A1 of record), in view of Newby et al. (US 5,796,829 of record), in further view of Tamer et al. (US 6,671,881 B1 of record) and Brooks et al. (US 5,973,684 of record).

As to claim 8, the claimed "wherein each said parameter comprises at least one byte of a section of a data packet to be received by the receiver/decoder" Note the Wasilewski et al reference discloses a receiver with a plurality of conditional access systems. Also note, the Wasilewski et al. reference discloses receiving a MPEG-2 transport stream (Wasilewski et al. [0131]; Provisional '575 [22:10-22]). However, the Wasilewski et al. reference does not specifically disclose the manner in which the transport stream is processed. Now note the Brooks et al. reference that discloses a digital entertainment terminal providing dynamic

execution in video dial tone networks wherein the digital entertainment terminal receives and processes MPEG-2 encoded information (Brooks 5:54-6:34). The Brooks et al. reference further discloses "[w]ithin a transport stream, a program association table (packet PID 0) maps each program source with the PID value associated with a program map table (PMT) related to that source...The program map, in turn, specifies the PID values for packets containing video, audio and/or data from the particular source" (Brooks 6:61-7:8) wherein PID values may represent video, audio, closed captioning, data, conditional access data (Brooks 6:44-60; 7:9-17). "Once the DET identifies and captures the program map table, the program decoder can extract the video elementary stream, the audio elementary stream(s) and any associated data stream for decoding of the programming" (Brooks 7:18-25). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Wasilewski et al. conditional access system with MPEG-2 transport streams with the Brooks identifiers of various data for the purpose of capturing and decoding particular programs within a MPEG-2 transport stream.

As to claims 9-11, please see rejection of claim 8.

As to claim 14, the claimed "wherein said manipulation means comprises a demultiplexer and a filter operable to filter specific components of data from the data received by the receiving means." Note the Wasilewski et al. reference discloses a MPEG-2 transport stream and demultiplexer (Wasilewski et al. [0062, 0131]; Provisional '575 [10:3-15,22:10-22]). However, the Wasilewski et al. reference does not specifically disclose how the MPEG-2 transport stream is processed. Now note the Brooks et al. reference that discloses a digital entertainment terminal providing dynamic execution in video dial tone networks. The Brooks et al. reference discloses

decryptor module decrypting the packets identified by appropriate PIDs [filtered], as directed by microprocessor, in the data stream, when authorized (Brooks 19:44-20:51). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wasilewski et al. conditional access system with MPEG-2 transport streams with the Brooks et al. decrypting of appropriate PID packets for the purpose of providing a means for decrypting and displaying particular programs within the transport stream.

As to claim 15, the claimed "wherein the manipulation protocol changes the filter so that only specific components of the data received by the receiving means are downloaded by the receiver/decoder" is met by the combination of claim 14, wherein DHCTSE controls access to transmitted programming wherein a selection of a different program would require modifying the filter to detect a new set of PIDs corresponding to the newly selected program.

As to claim 23, the claimed "wherein each said parameter comprises at least one byte of a section of a data packet to be received by the receiver/decoder" Note the Wasilewski et al reference discloses a receiver with a plurality of conditional access systems. Also note, the Wasilewski et al. reference discloses receiving a MPEG-2 transport stream (Wasilewski et al. [0131]; Provisional '575 [22:10-22]). However, the Wasilewski et al. reference does not specifically disclose the manner in which the transport stream is processed. Now note the Brooks et al. reference that discloses a digital entertainment terminal providing dynamic execution in video dial tone networks wherein the digital entertainment terminal receives and processes MPEG-2 encoded information (Brooks 5:54-6:34). The Brooks et al. reference further discloses "[w]ithin a transport stream, a program association table (packet PID 0) maps each program source with the PID value associated with a program map table (PMT) related to that

source...The program map, in turn, specifies the PID values for packets containing video, audio and/or data from the particular source" (Brooks 6:61-7:8) wherein PID values may represent video, audio, closed captioning, data, conditional access data (Brooks 6:44-60; 7:9-17). "Once the DET identifies and captures the program map table, the program decoder can extract the video elementary stream, the audio elementary stream(s) and any associated data stream for decoding of the programming" (Brooks 7:18-25). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Wasilewski et al. conditional access system with MPEG-2 transport streams with the Brooks identifiers of various data for the purpose of capturing and decoding particular programs within a MPEG-2 transport stream.

As to claims 24-26, please see rejection of claim 23.

As to claim 30, the claimed "wherein said at least one parameter comprises an identifier of a data packet to be received by the receiver/decoder." Note the Wasilewski et al and Newby et al. combination discloses a receiver with a plurality of conditional access systems with identifiers. Also note, the Wasilewski et al. reference discloses receiving a MPEG-2 transport stream (Wasilewski et al. [0131]; Provisional '575 [22:10-22]). However, the Wasilewski et al. reference does not specifically disclose the manner in which the transport stream is processed. Now note the Brooks et al. reference that discloses a digital entertainment terminal providing dynamic execution in video dial tone networks wherein the digital entertainment terminal receives and processes MPEG-2 encoded information (Brooks 5:54-6:34). The Brooks et al. reference further discloses "[w]ithin a transport stream, a program association table (packet PID 0) maps each program source with the PID value associated with a program map table (PMT)

related to that source...The program map, in turn, specifies the PID values for packets containing video, audio and/or data from the particular source" (Brooks 6:61-7:8) wherein PID values may represent video, audio, closed captioning, data, conditional access data (Brooks 6:44-60; 7:9-17). "Once the DET identifies and captures the program map table, the program decoder can extract the video elementary stream, the audio elementary stream(s) and any associated data stream for decoding of the programming" (Brooks 7:18-25). Therefore, the examiner submits that it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Wasilewski et al. and Newby et al. combination with the Brooks identifiers of various data for the purpose of capturing and decoding particular programs within a MPEG-2 transport stream.

As to claim 31, please see rejection of claim 30.

As to claim 32, please see rejection of claim 30.

As to claims 37-39, please see rejection of claims 30-32.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael W. Hoye whose telephone number is **571-272-7346**. The examiner can normally be reached on Monday to Friday from 8:30 AM to 5 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Miller, can be reached at **571-272-7353**.

Any response to this action should be mailed to:

Please address mail to be delivered by the United States Postal Service (USPS) as follows:

Mail Stop _____
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Effective January 14, 2005, except correspondence for Maintenance Fee payments, Deposit Account Replenishments (see 1.25(c)(4)), and Licensing and Review (see 37 CFR 5.1(c) and 5.2(c)), please address correspondence to be delivered by other delivery services (Federal Express (Fed Ex), UPS, DHL, Laser, Action, Purolater, etc.) as follows:

United States Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Some correspondence may be submitted electronically. See the Office's Internet Web site **http://www.uspto.gov** for additional information.

Or faxed to: 571-273-8300

Hand-delivered responses should be brought to the Customer Service Window at the address listed above.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to customer service whose telephone number is **571-272-2600**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see **http://pair-direct.uspto.gov**. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866-217-9197** (toll-free).

Michael W. Hoye
October 30, 2006

JOHN MILLER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600